They're B-A-A-C-K!!

Sooner or later, everything old is new again.
— Stephen King

Spring4Shell Bad Routers, the FBI, and you Id.me, The IRS, and me And These Clowns Are Back.

Each of the week's Topics #1 derives from what I detect is an unifying theme in IT news stories I read. Once developed, I use that theme to make a greater statement about where we are all at as we do our best to navigate the ever more complex digital world. What I noticed when looking at the news headlines as a whole over a 2 week span, the theme that developed, as I saw it, was many of the major themes discussed in this blog over the last 6 months have all come back in spades. And, as I was just settling in to begin writing out this theme, **a real oldie, but a goodie**, came back into the headlines.

"**Hackers hijack adult websites to infect victims with malware**" was the headline.

> **Cybercriminals are tricking victims into downloading malware by telling them their browsers are outdated and need to be updated in order to view the contents of the page.**
>
> **Avast cybersecurity researchers Jan Rubin and Pavel Novak uncovered a phishing campaign in which an unknown threat actor compromised more than 16,000 WordPress and Joomla hosted websites with weak login credentials.**
>
> **These are usually adult content websites, personal websites, university sites, and local government pages.**

Wordpress and Joomla are web development applications that make it easier for anyone to develop webpages. Both applications are constantly under threat, need ever vigilant updating, and are still a large attack surface. I have never used either application in developing webpages.

That is not, however, what got my attention. It was the porn sites aspect that got my attention. It seems like a very long time ago, but I discovered porn sites to be a very common source of malware. My common joke at the time was:" You want to watch porn? That's why god made DVDs."
You see, Sooner or later, everything old is new again.

Spring4Shell

How about that Java Library Vulnerability that was such the hot topic just 2 or 3 months ago? Well, Log4j/Log4Shell is still around, but as with so many topics of public discussion, it got blown off the news by the war. So not too many people have likely heard about there being another widely used Open Source Java application with a new set of Java based vulnerabilities and malware. **Researchers are also not in agreement what to call the new vulnerability, like they did at first with Log4j/Log4Shell.**

> **A concerning security vulnerability has bloomed in the Spring Cloud Function, which could lead to remote code execution (RCE) and the compromise of an entire internet-connected host.**
>
> **Some researchers have noted that because of its ease of exploit and Java-based nature, it's reminiscent of the Log4Shell vulnerability discovered in December.**
>
> **"[This] is another in a series of major Java vulnerabilities," Stefano Chierici, a security researcher at Sysdig, noted in materials shared with Threatpost. "It has a very low bar for exploitation so we should expect to see attackers heavily scanning the internet. Once found, they will likely install cryptominers, [distributed denial-of-service] DDoS agents, or their remote-access toolkits."**

Although extensive reporting among the digerati about the vulnerability was made, the story did not get much traction in the national media as far as I could tell. On April 1, Ars Technica declared "**Spring4Shell: The Internet security disaster that wasn't.**" Even criticizing early posters about this new Java vulnerability, who **"warned of severe damage the flaw might cause to "tonnes of applications" and claimed that the bug**

“can ruin the Internet” for being overtly hyperbolic. Much of the criticism was directed to security vendors. In language that might sound familiar to my readers, Ars Technica roasted these vendors for their obvious opportunism.

> **"Almost immediately, security companies, many of them pushing snake oil, were falling all over themselves to warn of the imminent danger we would all face. And all of that before a vulnerability tracking designation or advisory from Spring maintainers was even available."**

As I watched the news on this new vulnerability unfold, it did seem that another shoe was bound to drop. On April 4, the discussion indeed changed. Dark Reading reported that "**Millions of Installations Potentially Vulnerable to Spring Framework Flaw**."

> **Security firms produced two data points on Monday to estimate the number of Spring Framework installations that are vulnerable to the most recent flaw — CVE-2022-22965, also known as Spring4Shell or SpringShell — suggesting anywhere from hundreds of thousands to millions of instances are affected.**

And, in the course of a couple days, all of the earlier reporting, was roundly refuted.

> **"Given early reports suggest [SpringShell affected] around 6,000 devices, this new number is much worse," Smith says. "Log4j was much harder to assess whether an exposed port was using a Java-based application with Log4j behind the scenes. This is much more visible and directly available to exploit and test."**

Indeed, major computer companies, both hardware and software, reported the presence of SpringShell. "**Microsoft 365 Defender Threat Intelligence Team** also chimed in, stating it has been "tracking a low volume of exploit attempts across our cloud services for Spring Cloud and Spring Core vulnerabilities." On April 8, Microsoft had patched its vulnerable systems.

By April 5, **BleepingComputer** reported that "**Roughly one out of six organizations worldwide that are impacted by the Spring4Shell zero-day vulnerability have already been targeted by threat actors**."

By April 8, "**SpringShell was detected being actively exploited by threat actors to execute the Mirai botnet malware, particularly in the Singapore region since the start of April 2022,**" according to BleepingComputer. And this brings us full circle, with this vulnerability, which was first seemingly poo-pooed by all the important players, having maybe a more negative impact on regular computers users, like the readers of this post. SpringShell is weaponized:

> **This is far from the first time the botnet operators have quickly moved to add newly publicized flaws to their exploit toolset. In December 2021, multiple botnets including Mirai and Kinsing were uncovered leveraging the Log4Shell vulnerability to breach susceptible servers on the internet.**
>
> **Mirai, meaning "future" in Japanese, is the name given to a Linux malware that has continued to target networked smart home devices such as IP cameras and routers and link them together into a network of infected devices known as a botnet.**
>
> **The IoT botnet, using the herd of hijacked hardware, can be then used to commit further attacks, including large-scale phishing attacks, cryptocurrency mining, click fraud, and distributed denial-of-service (DDoS) attacks.**

As of reporting April 5, "**Data from Sonatype suggests that 80 percent of weekly Spring framework downloads are still exploitable versions**." With **"Patched versions of Spring are now available but a majority of developers are still downloading vulnerable iterations. " So I suggest you avoid the porn sites for awhile**.

Next on our list of everything old is new again, the subject just touched on above.

Back to Top

Bad Routers, the FBI, and You.

You might have heard that on Wednesday April 6, 2022, the **FBI announced the Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate (GRU).** Although the action itself was widely reported, what was not widely reported, but included in the Justice Department press release, was the fact that

> **"a two-tiered global botnet of thousands of infected network hardware devices under the control of a threat actor known to security researchers as Sandworm, which the U.S. government has previously attributed to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (the GRU).**

An "**infected network hardware device**" is a router that should either have been patched or replaced long ago. So it is not only me who is telling owners of old out of date networking gear, that you unknowingly represent a fifth column in our ongoing cyberwar with Russia. The court that agreed to issue the warrant to take down the botnet also apparently agreed with the statement above.

Later reporting in **Ars Technica**, was more specific about what and whose networking products were so affected.

> **The infected devices were primarily made up of firewall appliances from WatchGuard and, to a lesser extent, network devices from Asus. Both manufacturers recently issued advisories providing recommendations for hardening or disinfecting devices infected by the botnet, known as Cyclops Blink. It is the latest botnet malware from Russia's Sandworm, which is among the world's most elite and destructive state-sponsored hacking outfits.**

Ironically, or so it seems, WatchGuard, fixed its vulnerabilities here in May 2021, but didn't bother to tell too many about having done so. So even if your network admin was usually on the ball, if that person didn't know to patch, then they probably didn't patch. **"These issues were found by our engineers and not actively found in the wild. For the sake of not guiding potential threat actors toward finding and exploiting these internally discovered issues, we are not sharing technical details about these flaws that they contained**," said **WatchGuard in its May 2021** firmware update release.

Moreover, the past couple of weeks have not been kind to other vendors of networking gear and their customers. In February, Cisco Systems announced "**15 vulnerabilities affect routers used by small and medium-sized businesses (SMBs), businesses large and small are intertwined from a security perspective in 2022**." What is brought out in the Venture Beat article referenced above is the single most unsettling fact about vulnerabilities in equipment so widely used in businesses, both large and small, is that large scale enterprises will (eventually) patch, while smaller firms might not ever patch.

> **When an SMB doesn't address a major security issue such as this — due, for instance, to lack of resources — this can spill over into becoming a problem for the enterprises they do business with.**
>
> **"When SMBs get hacked, that can impact larger organizations," said Matthew Warner, cofounder and chief technology officer at Blumira, in an email.**

One of the central tenants of Zero Trust, and this reporter, is there are no boundaries to the network; or as I have put it more plainly: "There is only one network." So any vulnerability inherent within the system of any node of network (like your PC) is a vulnerability to the entire network.

And the the bad news on obsolete routers has continued apace. "**On April 4 2022, the Cybersecurity & Infrastructure Security Agency (CISA) added CVE-2021-45382 to its known exploited vulnerabilities catalog**. The affected routers were older D-Link models. "**But since the affected products have reached end of life (EOL), the advice is to disconnect them, if still in use**." **"D-Link lists the affected models that have reached EOL as DIR-810L, DIR-820L/LW, DIR-826L, DIR-830L, and DIR-836L all series and all hardware revisions. All of these models were offered a last update on 19 December 2021."** So if you have an older D-Link router, Uncle Sam and the manufacturer, are both asking you to replace it. I think this will sound familiar. Actually, I cannot remember the government ever before telling users to simply junk their old hardware.

On **April 1, 2022, ASUS released updates for 15 different models whose vulnerabilities were exploited by hackers working on behalf of the Russian Bear.** My experience tells me that users with ASUS routers are generally the least tuned into security issues and consider themselves simply consumers. So, will likely never patch their router, and as long as it connects to the Internet will not replace it.

All these unpatched, or unable to be patched, routers are simply sitting ducks of an attack surface, just waiting for the next criminal group to exploit them.

Back to Top

Id.me, The IRS, and me *(Ah jeez...)*

On the Dispatch Posted **February 13, 2022**, within the discussion introducing Zero Trust, there was a discussion of the short lived IRS experiment with Id.me. You may recall that there was an uproar across both parties in Congress, and the public at large. The post was timely. **On February 8, 2022, the IRS announced that the agency would cease using facial recognition for taxpayers to log into their IRS accounts**. This change was widely reported in the mainstream media, as well.

Except ID.me is still the gateway to your IRS online account, and requires a selfie. On **April 7, 2022, U.S. Senator Bob Menendez (D-N.J.) grilled the IRS Commissioner Charles Rettig about the IRS continued use if ID.me facial recognition technology.**

> **"I am also extremely concerned about the amount of information ID.me collects and stores for every taxpayer that uses its website—as a matter of fact as ID.me tells me according to this California disclosure in its notice for residents includes things like, age, gender, military/veteran status, and the taxpayers' location...where they access the ID.me website," added Sen. Menendez. "Even though tax returns and tax identity information—including a taxpayers' name, address, and taxpayer identification number—are protected from disclosure or potential disclosure by Internal Revenue Code section 6103, the information disclosed to ID.me is not protected."**

Senator Menendez has led the charge with over 200 other members of Congress to stop the collection of facial recognition and the shoddy reputation of ID.me. But no matter. Id.me remains the gatekeeper to your IRS account. I tried. It's really rotten technology.

I am entitled to a $619 tax return for year 2021. I don't ask. I just do the free online return. The refund may get all sucked up by back taxes. It is also possible the older taxes are past time for collection; and the newer taxes paid. Social Security was deducting for past taxes. And that stopped. Maybe because I met my obligation, or maybe because the IRS temporarily stopped collecting. So that is something I would like to know.

I find the selfie to be the epitome of narcissism. And they are usually very unflattering of those of us in advancing years. Then there is what I know about Id.me and its spotty history. Yes, there is an alternative to the Id.me facial recognition IRS logon clusterf**k. One can do a telephone interview of approximately 15 minutes in length. I was number 9 in the queue. If you do the a mathin' that's 135 minutes waiting for my 15 minute telephone interview. On hold waiting for 2 hours:15 minutes. Score ID.me debacle 1: Gerry 0. I did not gain access to my IRS account.

Back to Top

And These Clowns Are Back

In a post on **December 26, 2021**, I commented on a TV advertisement that I thought was a bit curious. The spot featured an actor dressed in blue jeans and a blue work shirt; and he was situated in a machine shop. The actor was the embodiment of the mythical Blue Collar Worker. And he was here to tell the world to tell Congress to not Send Our Tech Jobs To China, like had happened to his job. I pointed out the inconsistency of the ad's presentation. The guy looked like he was at work in the machine shop. What my main commentary was that it seemed like an issue advocacy ad, but there was no legislative proposal that the ad was promoting or attacking. The ad was pure FUD.

They are now back with the same message, but in different settings. If you read the fine print on the ad you will find that this is an organization called the **American Edge Project**. It turns out that this group is really just another Facebook facade, and the brain child of Mark Zuckerberg. As the headline in the Washington Post, **May 12, 2020**, stated "**Facebook is quietly helping to set up a new pro-tech advocacy group to battle Washington. The organization, called American Edge, arrives at a time when the industry is facing withering antitrust scrutiny in Washington**".

What the ads do not say is what this group was created to oppose is the truly bi-partisan effort in Congress to apply antitrust laws to the tech megacorps. Most noticeably, it is **Sen. Josh Hawley (R-MO) who has been most critical of Facebook and is its American Edge project**. There is no left vs right dichotomy at play here. If you look at who has lent their names to this Zuckerberg's little baby, you see that its "**Leadership**" is compromised mostly of has been milk toast politicians left of center to right of center. People whose only claim to fame now is, to quote Terry Malloy from **On The Waterfront**: "**I coulda been a contenda!"**

Of course, this has nothing to do with sending tech jobs to China. Nobody who works for Facebook is going to relocate to China because the coders may not be able to so blatantly manipulate the thoughts and emotions of impressionable teenage girls. We all saw the brutal crackdown of the remnants of free society in Hong Kong. China is not as much a pariah state as say, Russia is now, but no one who is concerned about free speech and free markets in the US is moving to China anytime soon.

Nevertheless, isn't this what Facebook is really all about. Playing on people's fears and emotions with vacuous claims and hysteria that wilt whenever the slightest amount of light is focused on their FUD. But this is not **Maya**. Not illusion. This is just plain old bullshit.

Beware of Maya

Beware of Darkness, George Harrison

Back to Top

Gerald Reiff